there is any doubt or dispute, it will be vital to emphasise that only a computer can respond rapidly enough to manage the threat posed by malware and that conventional law enforcement methods are incapable of doing so.

Only a lawful, appropriate, and reasonable self-help mechanism that is both immediate and devoid of technicalities and formalities can address issues like lack of harmonization, uncertainty about jurisdiction, absence of consistent extradition legislation between different nations, etc.

9) Limitations of the Study:

Potential research design or impact constraints, and statistical or data restrictions:

- Sample selection and the sample size is one the issue as this problem is not general in nature and a research scholar needs to contact secret agencies and the defense ministry to get key information concerning cyber terrorism that is quite not an easy job as it is related to national security.
- Data accessibility and dependability as well as the tools and procedures used to get the data is not an easy task for the researcher.
- Data from self-reporting
- The selection of research methods and methodology is one of the challenges.
- Time restrictions
- Cultural concerns and other matters can have an impact on studies.

10) Significance of the Study:

An increasing menace in today's society is cyberwarfare and cyberterrorism. Groups are becoming more conscious of the potential for cyberterrorism and warfare. There have been cyber-terrorist strikes throughout the past twenty years, and as time goes on and more and more countries become even more computerised, there will be an increase in these kinds of assaults.

It is wise to reevaluate the way that cyberterrorism and cyberwarfare are approached. Now is the moment to take action to safeguard both public and private strategic digital assets.

These systems must be constructed using technologies that have been tried and proved secure against the sophisticated threats[14] that are now being faced, as well as to plan as much as possible to deal with in the next years. If we can take action right away, we will not only be secure but also well-positioned to take advantage of the true potential of the digital revolution. Although netizens are digitally savvy, controlling the function of software developers and IT product firms is another part of preventative measure. We should make sure that firms that release such vulnerable software are held accountable and legally responsible. More serious sanctions should be applied when software tools are misused, necessitating control of the creation and distribution of such tools.

The risk is that once virus programmes are sold on the open market, they may be purchased and used by hackers anywhere in the globe. This is because it is getting simpler to conceal one's identity online.

It is the need of the time to have robust cyber regulations in India so that we can fight with every kind of cybercrime including cyberterrirism. It will not only protect our sovereignty but also save valuable human life and property.

[14] Technology and Terrorism : The New Threat for the Millennium - Leamington Spa, UK : RISCT. 24 p. Author(s): Bowers, Stephen R., Keys, Kimberly R